AO 106 (Rev. 04/10) Application for a Search Warrant

HH

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The residence located at 65311 Lake Road, Cambridge, Ohio 43725 including any curtilage and any/all persons, computers and/or digital media located therein

Case No. 2:19mj696

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT B INCORPORATED HEREIN BY REFERENCE

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT A INCORPORATED HEREIN BY REFERENCE

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC Secs 2252 and 2252A	Receipt/possession/distribution of child pornography/visual depictions of minors engaged in sexually explicit conduct in interstate commerce

The application is based on these facts:

SEE ATTACHED AFFIDAVIT INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

David A. Knight, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 9-10-19

Judge's signature

City and state: Columbus, Ohio

Chelsey M. Vascura, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

In the Matter of the Search of:	)	No. 2:19mj696
	)	
The residence located at	)	**Magistrate Judge**
65311 Lake Road, Cambridge, Ohio 43725	)	
including any curtilage, and any person or digital	)	
device located therein	)	

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, David A. Knight, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) assigned to the Cincinnati Division and I have been a Special Agent since August 2007. I am currently assigned to the FBI Child Exploitation Task Force, investigating matters involving the online exploitation of children and child pornography. Prior to joining the FBI, I was a Columbus, Ohio Police Officer for 8 years, also working on the FBI Child Exploitation Task Force. I have made arrests and have executed search warrants pertaining to these types of investigations.

2. During my career as a police officer and Special Agent, I have participated in various investigations involving computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, digital media, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses. As part of my duties as a Special Agent, I investigate criminal child exploitation and child pornography violations, including the illegal distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a) and 2252A.

3. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agents. I have

not included in this affidavit all information known by me relating to the investigation. I have set forth only the facts necessary to establish probable cause for a search warrant for the residential property located at **65311 Lake Road, Cambridge, Ohio 43725** (the SUBJECT PREMISES). I have not withheld any evidence or information that would negate probable cause.

5. The SUBJECT PREMISES to be searched is more particularly described in Attachment B, for the items specified in Attachment A, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2252 and 2252A – the distribution, transmission, receipt, and/or possession of child pornography. I am requesting authority to search the entire SUBJECT PREMISES, including the residential dwelling, any person located therein who may have a mobile computing device on his/her person, and any computer and computer-related media located therein where the items specified in Attachment A may be found, and to seize all items listed in Attachment A as instrumentalities, fruits, and evidence of crime.

III. APPLICABLE STATUTES AND DEFINITIONS

6. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce, or is in or affecting interstate commerce.

7. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

8. As it used in 18 U.S.C. § 2252, the term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2) (A) as: actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality;

masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.

9. As it is used in 18 U.S.C. § 2252A(a)(2), the term "child pornography"[1] is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

10. The term "sexually explicit conduct" has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), "sexually explicit conduct" also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated; (i) bestiality; (ii) masturbation; (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

11. The term "minor", as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as "any person under the age of eighteen years."

12. The term "graphic," as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean "that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted."

13. The term "visual depiction," as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image."

---

1 The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B hereto, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

14. The term "computer"[2] is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

IV. BACKGROUND REGARDING DIGITAL DEVICES, THE INTERNET AND MOBILE APPLICATIONS

15. I know from my training and experience that computer hardware, mobile computing devices, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.

16. Computers, mobile devices and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.

17. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including AGIF@ (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

18. Digital devices are also capable of storing and displaying movies of varying

[2] The term "computer" is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

19. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 32GB. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 4 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 4 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

20. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device

connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol ("IP") addresses[3] and other information both in computer data format and in written record format.

21. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography, or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user's true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.

22. It is often possible to recover digital or electronic files, or remnants of such files, months or sometimes even years after they have been downloaded onto a hard drive or other

---

3 The IP address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most ISPs control a range of IP addresses. When mobile devices connect to the Internet they are assigned an IP address either by the residential/commercial WiFi ISP or the cellular ISP. The IP address assignments are controlled by the respective provider.

digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

23. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

24. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

25. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

26. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as "apps," are

small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such "apps" include LiveMe, KIK messenger service, Snapchat, Meet24, and Instagram. LiveMe is a tool for broadcasting live-streaming videos and watching others' videos via smart device and personal computer through an internet connection. LiveMe allows users to use Instagram to promote live broadcasts, receive virtual gifts and convert them into real money rewards. Users of LiveMe can private message each other via the app and can share text, images, and videos during their chat conversations. Users of LiveMe log in with a phone number, Facebook account, or Instagram account. LiveMe also allows for groups or "Fams" to be created during which all members of a group can post messages, videos, and images that all other members can see and comment about.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

27. Searches and seizures of evidence from computers, mobile computing devices, and external storage media commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since

computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

28. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

29. In addition, there is probable cause to believe that any computer or mobile computing device and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2252 and 2252A, and should all be seized as such.

VI. SEARCH METHODOLOGY TO BE EMPLOYED

30. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth in Attachment A;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment A;

c. surveying various files, directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

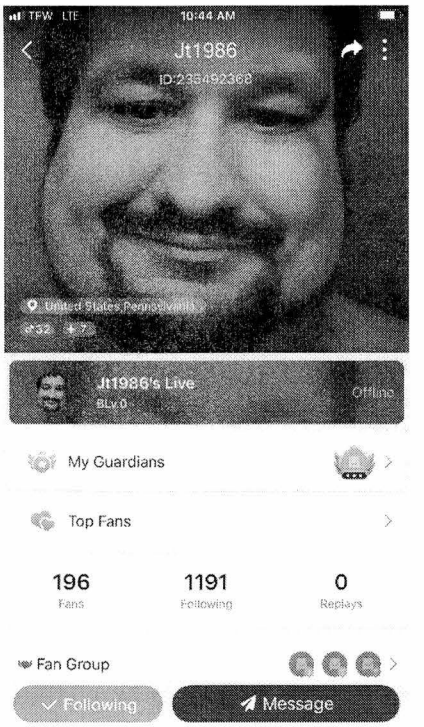
VII. INVESTIGATION AND PROBABLE CAUSE

A. Lead received from FBI Salt Lake City

31. In June of 2019, an undercover agent from Salt Lake City Division of the FBI was engaged in online chats via the application "Liveme". The undercover agent identified an individual with Liveme profile ID number 235492368 using the screen name "Jt1986" who is a member of a Liveme group entitled "Fun Times Fun Times" (hereinafter "the Chat Group"). The undercover agent was able to determine that members of the Chat Group were actively trading child pornography videos and images during their chats. The undercover agent was able to use recording software to document two trading sessions that occurred in the Chat Group on separate days. During the online sessions, Liveme user Jt1986 distributed child pornography to the Chat Group on several occasions.

32. Based on the activity that took place in the Chat Group, the undercover agent sent an administrative subpoena to Liveme and a follow-up subpoena to an internet service provider in an effort to identify Liveme user Jt1986. Based on information obtained in response to these subpoenas, the undercover agent ascertained that the user of the Liveme account Jt1986, was a Cambridge, Ohio resident and, as described below, is believed to be Joshua T. HAYNES (hereinafter HAYNES). The Salt Lake City Division provided your affiant with copies of the recorded undercover Liveme sessions with user Jt1986, information obtained from Liveme and the internet service provider in response to subpoenas, and results of law enforcement database checks pertaining to HAYNES. Based on your affiant's review of the material received from Salt Lake City Division, it is believed HAYNES is actively involved in child pornography offenses, as detailed below.

33. During the initial contact with HAYNES, the Salt Lake City undercover agent screen captured the Liveme profile for user Jt1986 (ID:235492368), which, as shown below, contained a profile picture of a white male with brown hair, goatee, and partial beard.



34. Your affiant reviewed the first chat session recorded by the undercover agent while in the Liveme Chat Group. The recording captured chat conversations that took place on June 21 and 22, 2019, and included several Liveme users. The recording showed that Jt1986 posted two photos on June 22, 2019, at 8:08 AM of what appeared to be a prepubescent female exposing her vagina to the camera and digitally penetrating herself. The female appears to be a minor and is wearing only a black t-shirt that says "ice cream". Further review of the chat recording showed that Jt1986 posted two photos of young girls on June 21, 2019, at 4:13 AM. The first photo depicted two clothed girls who appeared to be approximately 11-13 years of age, wearing revealing clothing and appearing to be about to kiss each other. The second photo depicted two clothed girls who also appeared to be approximately 11-13 years of age, taking a selfie in a mirror while standing in sexually provocative poses. Although these two photos did not depict child pornography, the children depicted were posed in a sexually provocative manner, and your affiant believes that the images are indicative of a sexual interest in children.

35. Also on June 21, 2019, at 1:46 AM, Jt1986 posted several more pictures to the chat room. All of the pictures depicted clothed females who appeared to be under the age of 18, wearing sexually revealing clothing and posing in a sexually provocative manner. One photo in particular depicted a young girl, approximately 12 years old, wearing jean shorts and a thin green tank top which is soaking wet. Through the tank top the young girl's underdeveloped breasts and

nipples were visible.

36. Your affiant also reviewed the second recording of the Liveme Chat Group conversation made by the undercover agent, which was created on June 24, 2019, and included chats from that date and several days prior. You affiant observed that, at 8:19 AM, on June 24, 2019, Jt1986 posted a video of an approximately 5-7 year old male, naked and visible only from the stomach down, laying on a bed that had a pink blanket with light pink polka dots. The video depicted an adult female performing fellatio on the naked male child.

37. Review of the earlier Chat Group conversations included in the second recording revealed that at 9:44 AM on June 22, 2019, a member of the group sent Jt1986 a message stating, "Hey I'm a perv dad, no limits, USA, hbu?" The next day at 2:44 PM, Jt1986 responded writing, "same to all," and then Jt1986 immediately started "following" the other Liveme member. Your affiant believes, based on training and experience, that Jt1986's statement "same to all" indicates that Jt1986 was claiming to also be a perv dad with no limits living in the USA. Your affiant is aware that men who have a sexual interest in children frequently refer to themselves as "perv" and use the phrase "no limits" to express their willingness to engage in sexual acts with children.

B. Records obtained from LiveMe and AT&T

38. On July 2, 2019, an administrative subpoena and preservation letter was served on LiveMe pertaining to user ID: 235492368 (username: Jt1986). Subscriber results were received in July of 2019, which included IP logs, Username, date of registration, last activity and sign-up platform: The results from Liveme are as follows:

Username:	Jt1986
Sex:	Male
Date of Registration:	2016-12-12
Last time of registration:	2019-7-1
Email:	joshee1986@gmail.com

39. Liveme provided multiple IP addresses that were utilized to access the Liveme account with user ID: 235492368. An administrative subpoena was sent to the two most recent and frequently used IP addresses in the Liveme results, which resolved to Frontier Communications. On July 8, 2019, Frontier Communications provided the following information:

- IP Addresses: 192.182.162.220 on 2019-05-20 and 192-182.169.254 on 2019-06-22
  Name: Ruth Hiles
  Address: 65311 Lake Drive, Cambridge, Ohio
  Email: shelbie_49@frontier.com
  Phone: 740-439-7207

(Note: The other IP addresses provided by Liveme resolve to wireless cell phone carrier Verizon Wireless. Your affiant is aware that Verizon would be unable to provide IP address information for the subscriber via administrative subpoena.)

C. Identification of Joshua T. HAYNES:

40. On August 22, 2019, your affiant conducted a check of the name Ruth Hiles in Lexis Nexis Accurint Law Enforcement (hereinafter Accurint LE) database. The database revealed that Ruth Hiles has a current listed home address of the SUBJECT PREMISES. Your affiant also discovered that the database lists Ruth Hiles as an associate of HAYNES, indicating that they are linked based on common addresses, phone numbers and/or other personal/biographical data. In this case, Accurint LE lists both Ruth Hiles and HAYNES residing at the SUBJECT PREMISES. Furthermore, your affiant ran HAYNES through Accurint LE and discovered that the SUBJECT PREMISES is listed as his current address.

41. On August 23, 2019 your affiant ran HAYNES through the Ohio Law Enforcement Gateway (OHLEG) which stores all driver's license information for the state of Ohio. HAYNES lists the SUBJECT PREMISES as his address on his current Ohio driver's license with his date of birth being 09/09/1986. Your affiant then compared HAYNES driver's license photo to the photo from the Jt1986 Liveme profile page. The photo from HAYNES' driver's license and the photo from Jt1986's Liveme profile page are the same person.

42. Additionally, open source queries for the Facebook page of "Joshua HAYNES, Cambridge, Ohio" revealed www.facebook.com/joshua.haynes.7902. A review of this Facebook page revealed pictures of HAYNES that match the pictures from both the driver's license photo of HAYNES and the Jt1986 Liveme profile picture.

43. In July 2019, FBI Task Force Officer (TFO) Brett Peachey communicated with Guernsey County Sheriff's Deputy Curtis Braniger about HAYNES. The deputy informed Peachey that he is familiar with HAYNES and he is planning to speak to HAYNES at the SUBJECT PREMISES about a bad check investigation. On July 24, 2019 Deputy Braniger confirmed that HAYNES lives at the SUBJECT PREMISES with his wife Ashley.

44. Therefore, based on the foregoing, your affiant believes HAYNES resides at the SUBJECT PREMISES, and that the instruments HAYNES uses to store and transmit child pornography, and to login to Liveme account Jt1986, will be discovered at the SUBJECT PREMESIS.

VI. COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST

IN CHILDREN

45. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in communicating about and engaging in sexual abuse of children and receiving, distribution or collecting child pornography:

A. Those who communicate about and engage in sexual abuse of children and exchange or collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature and communications about such activity.

B. Those who communicate about and engage in sexual abuse of children and trade or collect child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media, including digital files. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

C. Those who communicate about and engage in sexual abuse of children and trade or collect child pornography sometimes maintain any "hard copies" of child pornographic material that may exist that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These child pornography collections and communications are often maintained for several years and are kept close by, usually at the collector's residence. In some recent cases, however, some people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis, and to regularly delete any communications about the sexual abuse of children rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any

downloaded files have been deleted.

D. Those who communicate about and engage in sexual abuse of children and trade or collect child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

E. When images and videos of child pornography or communications about sexual abuse of children are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

46. In light of the statement that the user of the Jt1986 Liveme user made regarding being a "perv dad" with "no limits" and the pornographic and sexually suggestive nature of the images of minors that he posted to the Chat Group, your affiant believes that the user of the target Liveme account is a collector of child pornography. Based upon the conduct of individuals involved in trafficking in child pornography set forth in the above paragraphs, namely, that they tend to maintain their collections at a secure, private location for long periods of time, and that forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years after such evidence has been deleted from the computers or digital media, there is probable cause to believe that evidence of the offenses of receiving, distributing and possessing child pornography is currently located at the SUBJECT PREMISES, and will be recovered during forensic examination of any devices found within the SUBJECT PREMISES or on individuals located in the SUBJECT PREMISES.

VII. CONCLUSION

47. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 2252 and 2252A have been committed, and evidence of those violations is located in the residence of **65311 Lake Road, Cambridge, Ohio**

43725 and any computers, digital media and persons on whom a mobile computing device or cellular phone may be found, located therein. Your affiant respectfully requests that the Court issue a search warrant authorizing the search and seizure of the items described in Attachment A.

David A. Knight
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 10 day of ~~August~~ Sept, 2019.

Chelsey M. Vascura
United States Magistrate Judge
United States District Court, Southern District of Ohio

ATTACHMENT A
LIST OF ITEMS TO BE SEIZED

The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252 and 2252A.

The definition of child pornography contained in Section II of the attached Affidavit is incorporated herein by reference, and includes visual depictions of minors engaged in sexually explicit activity, as defined in 18 U.S.C. § 2256.

1. Computer(s), computer hardware (including but not limited to central processing units; internal and peripheral storage devices such as, external hard drives, floppy disk drives, diskettes, flash/thumb drives, and other memory storage devices), mobile computing devices, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest or sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to a sexual interest in children.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, online storage or chat programs), utilities, compilers, interpreters, and communications programs.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs, electronic

messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography.

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography and child erotica.

5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by cellular phone or computer, any child pornography.

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications related to the sexual abuse or exploitation of minors.

7. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider or Electronic Communications Service.

8. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.

9. Any and all cameras, film, videotapes or other photographic equipment, including cellular phones.

10. Any and all visual depictions of minors, for comparison to any child pornography or child erotica found during the execution of this search warrant or obtained during the course of this investigation.

11. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described in Attachment B, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

12. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.

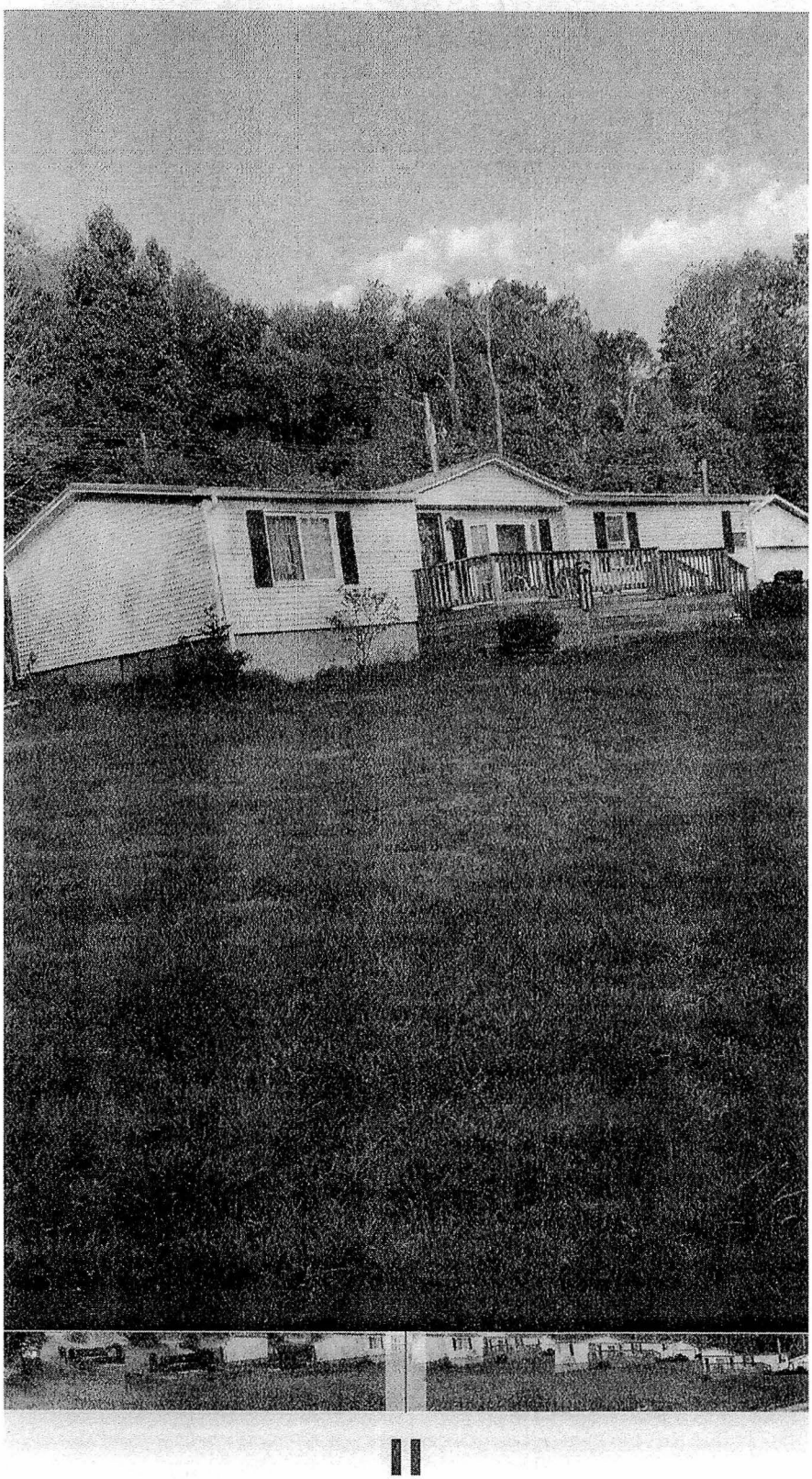
ATTACHMENT B
DESCRIPTION OF PLACE TO BE SEARCHED

The place to be searched is the residence described below, including all its appurtenances, parking areas, outdoor working areas, detached buildings, individuals at the residence who may be in possession of a digital storage or mobile computing device, and any computing related devices or digital media located therein or thereon.

The address **65311 Lake Road, Cambridge, Ohio 43725 (**depicted in the images below) is a single-story single-family double wide trailer. There is a white door in the rear of the residence with an attached wooden porch. The front of the residence has a brown door and brown storm door with a wooden front porch.

7:15

Today
7:13 AM



7:15

Today
7:13 AM